REDSHIFT NETWORKS

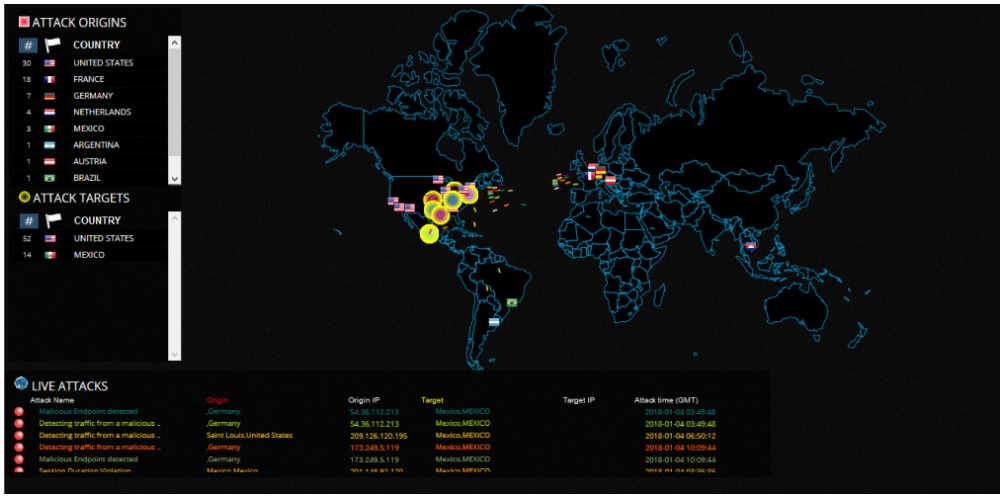
Unified Communication Threat Management

Market and Solution Overview

INTELLIGENTLY COMBINING SIP SECURITY, THREAT INTELLIGENCE ANALYTICS AND FRAUD DETECTION

Nearly $2 Trillion of telecom revenue is rapidly transitioning to IP/IMS/LTE/4G/5G/IoT with a critical dependence on real-time services and underlying VoIP and Unified Communications (UC) protocols including SIP and WebRTC. Like a sophisticated home alarm system, applying increasing levels of Security protection, Fraud prevention and Analytics insight are major priorities for these carrier UC services. Globally, carriers are spending more than $700B in network upgrades to support more than 6 Billion mobile users through VoIP/SIP/VoLTE VoIP services.

To securely deliver and monitor VoIP services for anomalous behavior, a new collective security approach is now available that leverages a proven in-depth security defense model via the RedShift Unified Communication Threat Management (UCTM) Platform. The UCTM platform intelligently combines SIP Security, Threat Intelligence Analytics and Fraud Detection to give operators real-time, context-driven visibility into unauthorized activities and mitigate threats including Denial of Service (DoS), Botnet attacks and Robocalls throughout their VoIP network.



Like scouting homes to break into, malicious hackers have a clear understanding of the edge (IP addresses) of most carrier networks. Typically, hijacking using DDoS, Botnets or Robocalls occurs from legitimate servers or even legitimately 'renting' the servers to initiate attacks often through the edge of SIP based networks (SBCs). 36 billion estimated SIP, VoLTE, VoIP and IoT endpoints are dependent upon secure carrier networks, including protection against anomalous network activity through VoIP Cyber-attacks, misconfigurations and network events.

Research from the RedShift Networks VoIP Threat Intelligence Network and Condor Labs research shows carriers and their enterprise customers now face more than 40,000 different VoIP/SIP attacks on a rapidly growing attack surface. UCTM easily identifies and vastly reduces these costly attack vectors and can proactively mitigate many of the VoIP service threats.

REDSHIFT NETWORKS

HOW DOES UCTM WORK?

UCTM applies real-time intelligence throughout VoIP system handshakes while video and audio calls are initiated from registered or remote video/phone systems. RedShift UCTM constantly inspects and monitors video edge device dial plans and security settings where hackers target call control edge devices and their internal connectivity to the switching infrastructure . RedShift's UCTM applies modern cybersecurity with VoIP underlying protocols including SIP, RTP, MS-SIP, TLS, SRTP and others. Hackers are unable to fraudulently disguise their presence over audio and video call traffic by using RedShift's UCTM real-time intelligent detection methods.

RedShift's VoIP security, fraud detection and threat intelligence analytics modules.

Security Module protects against more than 40,000 different VoIP threats & attacks

- Detection and auto-mitigation of Cyberprobes, Robocalls,DoS, Botnet attacks, and Registration Hijacking
- Exploitation of both known and unknown SIP vulnerabilities against well-known VoIP Devices - End Points/IP PBX/Softswitches/Softclients/Applications, etc.
- Provides a comprehensive and correlated Attack activity
- Real-time Global SIP/RTP Threat Intelligence and automatic blacklist updates

Fraud Detection & Prevention & Mitigation Module prevents anomalous traffic

- Blocks network-based preemptive attacks that result in Revenue Loss from Fraud
- Rich User Call Behavior Analytics with flexible rules
- Eliminates Toll Fraud activity, Subscriber fraud, VoIP fraud, PBX hacking, roaming fraud and Premium service frauds while ensuring 100% compliance of all SIP traffic

Advanced Analytics and Automation Module

- Provides rich advanced contextual driven analytics at the three VoIP/UC layers; Network layer, Application layer, and User layers (SIP/UC focused)
- Automates rich forensic and troubleshooting/debugging capabilities
- Details SIP Call Ladder Diagrams, Error Codes, UA, Active Sessions, Call Recording, etc.
- Identifies top services used, areas of SIP network under stress, networks that show suspicious/anomalous activities, etc.

WHO'S USING UCTM?

RedShift's global carrier customer base includes Tier 1, Tier 2 and Tier 3 operators offering fixed line, cable, Mobile, VoIP/UC and other OTT services. These customers use the UCTM to eradicate four problem areas:

- Stopping more than $29 billion in Fraudulent theft of UC services
- Limiting the $2.5 million spent on every telecom DDoS (TDDoS) attack
- Blocking the $9.5 billion spent on Robocalls
- Reducing the $15 billion lost annually on carrier network issues and VoIP troubleshooting.

Globally, carriers will spend more than $770 billion on expanding LTE and 5G upgrades to their networks. Typically, 4% to 8% of a network infrastructure project is spent on security resulting in a 10x ROI. RedShift will help carriers boost their VoIP service ROI, harden VoIP service security and provide actionable granular insight on anomalous traffic before it causes millions in dollars of lost or stolen service revenue.

RedShift Networks sells its UCTM solution, including the VoIP Threat Intelligence Network updates and Condor Labs research, direct and through global Resellers. The company has Marketing and Sales partnerships with Gigamon, Splunk, Polycom, Extreme Networks and others, The company's UCTM patented product has received several awards including SC Magazine Finalist 2016, Red Herring Global 100, Tie50, Product of the Year – Internet Telephony, Spiffy Award finalist; Speaker at SIPNOC, CFCA forum, and the Telecom Exchange & Telecom Council of Silicon Valley. Please visit www.redshiftnetworks.com for additional information.